

**CLAIMS:**

- 1           1.       A method of processing a message for authentication, said method  
2 comprising:  
3           performing a single iteration of a compression function using a key and said  
4 message as inputs when said message fits within an input block of said compression  
5 function; and  
6           using a hash function nested within a keyed hash function to process said  
7 message when said message does not fit within an input block of said compression  
8 function.
- 1           2.       The method of claim 1 wherein said step of using comprises the steps  
2 of:  
3           providing a first portion and a second portion of said message;  
4           performing a hash function using said first portion as an input to achieve a  
5 result; and  
6           performing a keyed hash function using said second portion and said result as  
7 inputs.
- 1           3.       The method of claim 2 wherein said hash function is an iterated hash  
2 function F and said keyed hash function is a keyed compression function f.
- 1           4.       The method of claim 2 wherein said hash function is an iterated hash  
2 function F and said keyed hash function is an iterated hash function F.
- 1           5.       The method of claim 1 further comprising the steps of:  
2           using a result from said compression function to produce a message  
3 authentication code; and

4            sending said message authentication code in association with said message for  
5            authenticating said message using said message authentication code.

1            6.        The method of claim 1 further comprises:  
2            using a result from said compression function to produce a message  
3            authentication code; and  
4            comparing said message authentication code to a received message  
5            authentication code received with said message, whereby said message is authentic if  
6            said message authentication code and said received authentication code match.

1            7.        A method of processing a message for authentication, said method  
2            comprising:  
3            providing a first portion and a second portion of said message;  
4            performing a hash function using said first portion as an input to achieve a  
5            result; and  
6            performing a keyed hash function using said second portion and said result as  
7            inputs.

1            8.        The method of claim 7 comprising the step of:  
2            determining whether said message fits within an input block of a compression  
3            function; and  
4            performing said steps of providing, performing and performing when said  
5            message does not fit within an input block of said compression function.

1            9.        The method of claim 7 comprising the step of:  
2            determining whether said message fits within an input block of a compression  
3            function; and

4 performing a single iteration of a compression function using a key and said  
5 message as inputs when said message fits within an input block of said compression  
6 function.

1 10. The method of claim 7 wherein said hash function is an iterated hash  
2 function F and said keyed hash function is a keyed compression function f.

1 11. The method of claim 7 wherein said hash function is an iterated hash  
2 function F and said keyed hash function is an iterated hash function F.

1 12. The method of claim 7 further comprising the steps of:  
2 using a result from said keyed hash function to produce a message  
3 authentication code; and  
4 sending said message authentication code in association with said message for  
5 authenticating said message using said message authentication code.

1 13. The method of claim 7 further comprises:  
2 using a result from said keyed hash function to produce a message  
3 authentication code; and  
4 comparing said message authentication code to a received message  
5 authentication code received with said message, whereby said message is authentic if  
6 said message authentication code and said received authentication code match.

1 14 A message authentication system comprising:  
2 processing circuitry configured to perform a single iteration of a compression  
3 function using a key and said message as inputs when said message fits within an  
4 input block of said compression function and to use a hash function nested within a  
5 keyed hash function to process said message when said message does not fit within an  
6 input block of said compression function.

1           15.    The system of claim 14 wherein said processing circuitry configured to  
2 provide a first portion and a second portion of said message, perform a hash function  
3 using said first portion as an input to achieve a result, and perform a keyed hash  
4 function using said second portion and said result as inputs.

1           16.    A message authentication system comprising:  
2           processing circuitry configured to provide a first portion and a second portion  
3 of said message, perform a hash function using said first portion as an input to  
4 achieve a result, and perform a keyed hash function using said second portion and  
5 said result as inputs.

1           17.    The system of claim 16 wherein said processing circuitry configured to  
2 determine whether said message fits within an input block of a compression function.

1           18.    The system of claim 17 wherein said processing circuitry configured to  
2 perform a single iteration of a compression function using a key and said message as  
3 inputs when said message fits within an input block of said compression function.